## B5.3-R4: NETWORK MANAGEMENT & INFORMATION SECURITY

**NOTE:**

> **1. Answer question 1 and any FOUR from questions 2 to 7.**
> **2. Parts of the same question should be answered together and in the same sequence.**

**Time: 3 Hours** **Total Marks: 100**

**1.**

a) Cryptographic algorithms and protocols can be grouped into four main areas. Explain all the areas with example.

b) Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101} in AES:

i) Show the original contents of State, displayed as a 4 × 4 matrix.
ii) Show the value of State after initial AddRoundKey.
iii) Show the value of State after SubBytes.
iv) Show the value of State after ShiftRows.
v) Show the value of State after MixColumns.

c) A cryptographic attack is a method for circumventing the security of a cryptographic system by finding a weakness Differentiate between brute force and dictionary attack.

d) List the business requirements of Secure Electronic Transaction (SET).

e) How does access control work at a number of levels like application, middleware, operating system and hardware in system?

f) Differentiate between authentication and authorization?

g) What are the possible ways to approach the identification of threats?

**(7x4)**

**2.**

a) What's the difference between an access control method, security model, and security policy?

b) Encode the message "This is a test" using the following encoding system:

i) Radix-64
ii) Quoted-printable

c) Modes of operation have been devised to encipher text of any size employing Data Encryption Standard (DES). Explain Cipher Block Chaining (CBC) mode. What about error propagation in it? What is cipher text stealing?

**(3+8+7)**

**3.**

a) What is Transport Layer Security (TLS)? Explain how mail server, database server, or directory server can be secured with TLS?

b) In theory, biometrics is a great way to authenticate a user. List the pros and cons of biometric authentication.

c) Why does key distribution process need a key distribution center? What is certification authority? Explain certification revocation list method.

**(6+5+7)**

**4.**

a) List the ways to combat Viruses, Worms and Trojan Horses on the computer.

b) What is stream cipher? Write the comparisons between stream ciphers and block ciphers?

c) Why prime numbers are used in RSA algorithm? In RSA, given e = 13 and n = 100:
Encrypt the message "How are you" using 00 to 25 for letter A to Z and 26 for the space. Use different blocks to make P < n.

**(5+5+8)**

**5.**

a) What is MD5? What are the differences between MD5 and SHA? What are a collision attack and a preimage attack?

b) What is a network firewall? List the critical resources in a firewall? What can not a firewall protect against that do not go through the firewall?

c) Define security policy and explain its purpose with relation to IPSec.

**(6+6+6)**

**6.**

a) List the Strength of RC4. Compare RC4 and RC5 stream cipher algorithm.

b) What is buffer overflow? Explain the ways to prevent buffer overflow? How to spoof IP address to conceal the online user's identity?

c) Write Steps to improve Security Incident Handling.

**(5+8+5)**

**7.**

a) Cryptanalysis is the science and art of breaking the codes. Explain various cryptanalysis attacks with example.

b) List and explain Virtual Private Network (VPN) protocols.

c) What is TCP session hijacking? Write steps to hijack TCP session.

**(6+6+6)**